

16 equipment.

1 18. The cryptographic communication system according to claim 17
2 wherein:

3 (1) said IC card further includes a receiver for receiving said
4 challenge data generated by said authentication equipment and transmitted via said
5 intermediary equipment, and a response data transmitter for transmitting said
6 encrypted data representing response data, said IC card ID data, and said
7 certificate of individual IC card key data to said authentication equipment via said
8 intermediary equipment;

9 (2) said means for producing said secret key in said authentication
10 equipment includes a storage unit for storing a validation key, a second
11 decryption unit for producing an IC card ID and a secret key by decrypting said
12 certificate of individual IC card key data received from said IC card, using said
13 validation key; and

14 (3) said authentication equipment further includes a challenge data
15 generator / storage unit for generating and storing said challenge data, and a
16 second matching determination unit for determining if said response data
17 decrypted by said first decryption unit matches with said challenge data stored in
18 said challenge data generator / storage unit.

1 19. The cryptographic communication system according to claim 18
2 wherein:

3 (1) said IC card further includes a combiner for generating
4 combined data by combining said IC card ID data, said certificate of individual IC
5 card key data, and said encrypted data, and transmitting said combined data to
6 said authentication equipment; and

(2) said authentication equipment further includes a first divider for dividing said combined data received from said IC card into said IC card ID data, said certificate of individual IC card key data, and said encrypted data, and a second divider for dividing data decrypted by said second decryption unit into said IC card ID and said secret key.

20. The cryptographic communication system according to claim 19 wherein said authentication equipment further includes a first combiner for combining said challenge data stored in said challenge data generator / storage unit and said IC card ID data produced by said second divider, a third divider for producing said challenge data from data combined by said first combiner, a second combiner for combining said response data decrypted by said first decryption unit and said IC card ID data produced by said second divider, and a fourth divider for producing said response data from data combined by said second combiner.

21. An electronic toll collection ("ETC") authentication system including an IC card, roadside equipment, and central processing equipment, comprising:

(1) said IC card including an encryption means for receiving a challenge data generated by roadside equipment, as said IC card passes said roadside equipment, and for encrypting said challenge data using a secret key; an encrypted data storage means for storing data encrypted by said encryption means; a response data transmission means for transmitting IC card ID data and a certificate of individual IC card key, together with said encrypted data stored in said encrypted data storage means, as response data to said roadside equipment;

(2) said roadside equipment including a dividing means for dividing said transmitted response data ; a second decryption means for decrypting said

13 certificate of individual IC card key data divided by said dividing means, using a
14 validation key; a first matching determination means for making a matching
15 determination of said IC card ID produced as a result of decryption with another
16 IC card ID provided by said dividing means; a first decryption means for
17 producing response data by decrypting an encrypted data provided by said
18 dividing means; and a challenge data transmission means for transmitting said
19 challenge data to said IC card; and

20 (3) said central processing equipment including challenge data
21 storage means for storing said challenge data generated by said roadside
22 equipment; and a second matching determination means for receiving said
23 response data decrypted by said first decryption means, and executing a matching
24 determination of said response data with said challenge data stored in said
25 challenge data storage means,

26 said ETC authentication system providing authentication of said IC
27 card ID by said roadside equipment by authenticating signature information
28 received with said IC card ID, and said central processing equipment providing a
29 matching determination of said response data encrypted by said IC card and
30 decrypted by said roadside equipment.

1 22. An electronic toll collection ("ETC") authentication method
2 comprising the steps of:

3 (1) encrypting challenge data using a secret key in an IC card, said
4 challenge data being generated by roadside equipment and transmitted to said IC
5 card when said IC card passes by said roadside equipment;

6 (2) storing said encrypted data;

7 (3) transmitting an IC card ID data and a certificate of individual IC

8 card key data, in addition to said stored encrypted data, as response data to said
9 roadside equipment;

10 (4) dividing said response data received by said roadside equipment
11 ;

12 (5) decrypting said certificate of individual IC card key data,
13 provided by the dividing step, using a validation key;

14 (6) carrying out a matching determination of an IC card ID provided
15 in the decrypting step with another IC card ID provided in the dividing step;

16 (7) providing a response data by decrypting said encrypted data
17 provided in the dividing step; and

18 (8) carrying out in said central processing equipment a matching
19 determination of said response data decrypted by said roadside equipment with
20 said challenge data,

21 said ETC authentication method providing authentication of said IC
22 card ID by said roadside equipment by authenticating signature information
23 received with said IC card ID, and said central processing equipment providing a
24 matching determination of said response data encrypted by said IC card and
25 decrypted by said roadside equipment.

1 23. An electronic toll collection ("ETC") authentication system
2 comprising:

3 (1) first roadside equipment including challenge data and time
4 generator / storage means for generating and storing challenge data and time
5 information, and transmitting said challenge data and time information to an IC
6 card;

(2) said IC card including an ID transmission means for transmitting an IC card ID before said IC card passes said first roadside equipment; an encryption means for receiving said challenge data and said time information generated by said first roadside equipment, as said IC card passes said first roadside equipment, and encrypting received data using a secret key; a response data transmission means for transmitting an IC card ID data and a certificate of individual IC card key data, together with said encrypted data as a response data to a second roadside equipment;

(3) said second roadside equipment including a first dividing means for dividing said response data ; a second decryption means for decrypting said certificate of individual IC card key data divided by said first dividing means, using a validation key; a first matching determination means for providing a matching determination of an IC card ID produced as a result of decryption with another IC card ID provided by said first dividing means; and a first decryption means for producing a response data by decrypting an encrypted data obtained from said first dividing means; and

(4) central processing equipment including a second dividing means for dividing said challenge data and said IC card ID generated by said first roadside equipment; a third dividing means for dividing said response data and said IC card ID decrypted by said second roadside equipment; and a second matching determination means for making a matching determination of said challenge data obtained by said second dividing means and said response data provided by said third dividing means,

said ETC authentication system providing authentication of said IC card ID by said second roadside equipment by authenticating signature information received with said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC

34 card and decrypted by said second roadside equipment.

1 24. The ETC authentication system according to claim 23, wherein
2 said second roadside equipment further comprises another decryption means for
3 decrypting said encrypted data provided by said first dividing means, using a
4 secret key reproduced by said second decryption means; and a validation means
5 for providing time information, at which said IC card passed said first roadside
6 equipment, from a decrypted result of said another decryption means, and for
7 confirming if a difference between said time information and present time is
8 within a predetermined time period.

1 25. An electronic toll collection ("ETC") authentication method
2 comprising the steps of:

3 (1) receiving a card ID from an IC card before said IC card passes
4 first roadside equipment;

5 (2) encrypting challenge data and time information using a secret
6 key, said challenge data and time information being generated by first roadside
7 equipment and transmitted to said IC card when said IC card passes said first
8 roadside equipment;

9 (3) transmitting IC card ID data and a certificate of individual IC
10 card key data, in addition to said encrypted data, as a response data to second
11 roadside equipment;

12 (4) dividing said transmitted response data in said second roadside
13 equipment;

14 (5) decrypting said certificate of individual IC card key data
15 provided in the dividing step using a validation key;

16 (6) carrying out a matching determination of an IC card ID provided
17 in the decryption step with another IC card ID provided in the dividing step;

18 (7) providing a response data by decrypting said encrypted data
19 provided in the dividing step;

20 (8) carrying out in central processing equipment a matching
21 determination of said challenge data provided from said first roadside equipment
22 and said response data decrypted in said second roadside equipment,

23 said ETC authentication method providing authentication of said IC
24 card ID by said second roadside equipment by authenticating signature
25 information received with said IC card ID, and said central processing equipment
26 providing the matching determination of said response data encrypted by said IC
27 card and decrypted by said second roadside equipment.

1 26. The ETC authentication method according to claim 25 further
2 comprising the steps of:

3 (1) decrypting said encrypted data provided by the dividing step,
4 using a secret key reproduced in said decryption step; and

5 (2) providing time information, at which said IC card passed said
6 first roadside equipment, as a result of the decryption step, and confirming if a
7 difference between said time information and present time is within a
8 predetermined time.

1 27. An electronic toll collection ("ETC") authentication system
2 comprising:

3 (1) a first roadside equipment including a challenge data generation
4 means for generating a challenge data, and transmitting said challenge data to an

5 IC card;

6 (2) said IC card including an ID transmission means for transmitting
7 an IC card ID before said IC card passes said first roadside equipment; an
8 encryption means for receiving said challenge data generated by said first
9 roadside equipment, as said IC card passes said first roadside equipment, and
10 encrypting said challenge data using a secret key; and a response data
11 transmission means for transmitting an IC card ID data and a certificate of
12 individual IC card key data, together with said encrypted data as response data to
13 second roadside equipment;

14 (3) said second roadside equipment including a first dividing means
15 for dividing said response data; a decryption means for decrypting said certificate
16 of individual IC card key data divided by said first dividing means, using a
17 validation key; a first matching determination means for providing a matching
18 determination of said IC card ID produced as a result of decryption with another
19 IC card ID provided by said first dividing means; and a first decryption means for
20 decrypting an encrypted data provided by said first dividing means to obtain
21 response data;

22 (4) central processing equipment including a second dividing means
23 for dividing said challenge data and said IC card ID generated in said first
24 roadside equipment; a third dividing means for dividing said response data
25 decrypted in said second roadside equipment and said IC card ID; and a second
26 matching determination means for providing a matching determination of said
27 challenge data obtained in said second dividing means and said response data
28 obtained in said third dividing means,

29 said ETC authentication system providing authentication of said IC
30 card ID by said second roadside equipment by authenticating signature

31 information received with said IC card ID, and said central processing equipment
32 providing the matching determination of said response data encrypted by said IC
33 card and decrypted by said second roadside equipment.

1 28. An electronic toll collection ("ETC") authentication method
2 comprising the steps of:

3 (1) receiving a card ID from an IC card before said IC card passes
4 by first roadside equipment;

5 (2) encrypting a challenge data using a secret key, said challenge
6 data being generated by said first roadside equipment and transmitted to said IC
7 card when said IC card passes said first roadside equipment;

8 (3) transmitting each individual data of said IC card ID and a
9 certificate of individual IC card key, in addition to said challenge data encrypted
10 in the encryption step, as response data to second roadside equipment;

11 (4) dividing said response data transmitted in the transmission step by
12 said second roadside equipment;

13 (5) decrypting said certificate of individual IC card key data divided
14 in the dividing step, using a validation key;

15 (6) carrying out a matching determination of said IC card ID
16 produced as a result of decryption with another IC card ID provided by the
17 dividing step;

18 (7) producing a response data by decrypting said encrypted data
19 provided by the dividing step; and

20 (8) executing in central processing equipment a matching
21 determination of said challenge data provided by said first roadside equipment and

22 said response data decrypted by said second roadside equipment,
23 said ETC authentication method providing authentication of said IC
24 card ID by said second roadside equipment by authenticating signature
25 information received said IC card ID, and said central processing equipment
26 providing the matching determination of said response data encrypted by said IC
27 card and decrypted by said second roadside equipment.

2025 RELEASE UNDER E.O. 14176